INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA SINTÉTICO

UNIDAD ACADÉMICA: UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERÍA Y TECNOLOGÍAS AVANZADAS

PROGRAMA ACADÉMICO: Ingeniería Telemática

UNIDAD DE APRENDIZAJE: Criptografía **NIVEL:** III

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE:
Genera sistemas informáticos seguros con base en algoritmos criptográficos, tanto en software como en hardware y en sus protocolos.

CONTENIDOS:

I. Introducción a la criptografía.
II. Criptografía de clave simétrica.
III. Criptografía de clave asimétrica.
IV. Fundamentos matemáticos de funciones Hash.
V. Fundamentos matemáticos de firmas digitales

ORIENTACIÓN DIDÁCTICA:

Esta unidad de aprendizaje se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico, deductivo, comparativo y activo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, trabajos de investigación, organizadores gráficos, programas de cómputo, discusión guiada y prácticas de laboratorio.

EVALUACIÓN Y ACREDITACIÓN:

La presente Unidad de Aprendizaje se evaluará a partir del esquema de portafolio de evidencias, el cual se conforma de: evaluación diagnóstica, evaluación formativa, sumativa y rubricas de autoevaluación y coevaluación.

Esta unidad de aprendizaje también se puede acreditar mediante:

- Evaluación de saberes previamente adquiridos, con base en los criterios establecidos por la Academia.
- Acreditación en otra unidad académica del IPN u otra institución educativa, nacional o internacional, externa al IPN, con la cual se tenga convenio.

BIBLIOGRAFÍA:

- Ferguson, Niels, Schneier, Bruce and Kohno Tadayoshi (2010). Cryptography Engineering: Design Principles and Practical Applications (1st Edition). USA: Wiley. ISBN: 978-0-470-47424-2.
- Mollin, Richard (2007). An introduction to Cryptography (2nd Edition). USA Taylor & Francis. ISBN: 978-1-58488-618-1.
- Paar, Christof, Pelzl, Jan and Preneel, Bart (2010). Understanding Cryptography: A Textbook for Students and Practitioners (2nd Edition). Germany: Springer. ISBN: 978-3-642-04100-6.
- Hans Delfs, Helmut Knebl (2007), Introduction to Cryptography. Principles and Applications (2nd Edition). USA: Springer. ISBN: 978-3-540-49243-6.
- Wade Trappe, Lawrence C. Washington (2006). Introduction to Cryptography with Coding Theory (2nd Edition). USA: Pearson Prentice Hall. ISBN: 978-0-131-86239-5.

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

UNIDAD ACADÉMICA: Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas.

PROGRAMA ACADÉMICO: Ingeniería Telemática

SALIDA LATERAL: N/A

ÁREA FORMACIÓN: Profesional

MODALIDAD: Escolarizada

UNIDAD DE APRENDIZAJE: Criptografía

TIPO DE UNIDAD DE APRENDIZAJE: Teórico – práctico/optativa

VIGENCIA: Agosto 2012

NIVEL: III

CRÉDITOS: 7.5 Tepic - 4.56 SATCA

INTENCIÓN EDUCATIVA

Esta unidad de aprendizaje contribuye a conformar el perfil de egreso del Ingeniero Telemático desarrollando destrezas para resolver problemas que involucren el uso de algoritmos criptográficos para aplicaciones específicas en los protocolos de comunicación. Además, desarrolla las siguientes competencias: resolución de problemas, toma de decisiones, trabajo en equipo, presentación de la información, fomenta la tolerancia, la creatividad y la responsabilidad.

Las unidades de aprendizaje relacionadas son como precedentes álgebra lineal, probabilidad, programación y programación avanzada; y la consecuente es seguridad de datos.

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Genera sistemas informáticos seguros con base en algoritmos criptográficos, tanto en software como en hardware y en sus protocolos.

TIEMPOS ASIGNADOS

HORAS TEORÍA/SEMANA: 3.0

HORAS PRÁCTICA/SEMANA: 1.5

HORAS TEORÍA/SEMESTRE: 54.0

HORAS PRÁCTICA/SEMESTRE: 27.0

HORAS TOTALES/SEMESTRE: 81.0

UNIDAD DE APRENDIZAJE DISEÑADA POR: Academia de Telemática

REVISADA POR: Subdirección Académica

APROBADA POR: Consejo Técnico Consultivo Escolar.

S. E. P.

M. en C. Arodi Rafael Carvallo Domínguez
Presidente del CTCE
14 de Diciembre de 2011

AUTORIZADO POR: Comisión de Programas Académicos del Consejo General Consultivo del IPN

M. en C. Daffny Rosado Moreno
Coordinador de la Comisión de Programas Académicos
11 de Abril de 2012

N° UNIDAD TEMÁTICA: I **NOMBRE:** Introducción a la criptografía

UNIDAD DE COMPETENCIA

Bosqueja un sistema seguro, las aplicaciones de la criptografía y criptosistemas clasicos con base en la teoria de numeros.

No	CONTENIDOS	HORAS AD Actividades de Docencia		HORAS TAA Actividades de Aprendizaje Autónomo		CLAVE BIBLIOGRÁFICA
		T	P	T	P	
1.1.	Introducción a las comunicaciones seguras	0.5		1.0		1B,2B,3C,4B,5C, 6B,7B
1 2 1.2.1 1.2.2	Criptología Criptografía Criptoanálisis	1.0		1.0		
1 3	Aplicaciones de la criptografía	0.5		1.0		
1 4 1.4.1 1.4.2 1.4.3	Criptosistemas clásicos Cifrador por corrimiento Cifrador afín Cifrador Vigenère	2.0	1.5	2.5		
1.5 1.5.1 1.5.2 1.5.3	Fundamentos de teoría de números Congruencias y aritmética modular Teorema de Fermat y de Euler Campos finitos	2.5	1.5	2.5	1.0	
	Subtotales:	6.5	3.0	8.0	1.0	

ESTRATEGIAS DE APRENDIZAJE

Encuadre del curso

La unidad temática se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico, deductivo, comparativo y activo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, discusión guiada y las prácticas de laboratorio I y II.

EVALUACIÓN DE LOS APRENDIZAJES

Portafolio de evidencias:

Evaluación diagnóstica	
Autoevaluación y coevaluación (rúbrica)	
Resolución de problemas	25%
Reporte de mesa redonda	5%
Evaluación escrita	35%
Reportes de las prácticas	35%

UNIDAD DE APRENDIZAJE: Criptografía

Nº UNIDAD TEMÁTICA: II **NOMBRE**: Criptografía de clave simétrica

UNIDAD DE COMPETENCIA

Estructura aplicaciones de criptografía de clave simétrica con base en los algoritmos de cifrado DES, AES y modos de operación como CBC, CFB y OFB.

No.	CONTENIDOS	HORAS AD Actividades de Docencia		HORAS TAA Actividades de Aprendizaje Autónomo		CLAVE BIBLIOGRÁFICA
		T	P	T	P	
2.1	Conceptos	0.5		1.0		1B, 2B,3C,4B, 6B,8C,10C,11C
2.2 2.2.1. 2.2.2.	Estándar de cifrado de datos (DES) Seguridad de DES Ataques para DES	0.5		0.5	1.5	
2.3 2.3.1. 2.3.2. 2.3.3.	Estándar avanzado de cifrado (AES) Capas de AES Seguridad de AES Ataques para AES	1.0	2.0	2.5	1.5	
2.4 2.4.1 2.4.2 2.4.3	Modos de operación Modo de cifrado a bloques encadenado (CBC) Modo de cifrado por retroalimentación (CFB) Modo de cifrado con retroalimentación a la salida (OFB)	1.0	1.0	2.0	2.0	
	Subtotales:	3.0	3.0	6.0	5.0	

ESTRATEGIAS DE APRENDIZAJE

La unidad temática se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico, comparativo y activo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, discusión guiada, organizadores gráficos y las prácticas de laboratorio III y IV

EVALUACIÓN DE LOS APRENDIZAJES

Portafolio de evidencias:

Problemas resueltos	25%
Mapas conceptuales	5%
Evaluación escrita	35%
Reportes de las prácticas	35%
Autoevaluación y coevaluación (rúbrica)	

UNIDAD DE APRENDIZAJE: Criptografía

N° UNIDAD TEMÁTICA: III **NOMBRE**: Criptografía de clave asimétrica

UNIDAD DE COMPETENCIA

Estructura programas de criptografía de clave asimétrica con base en los algoritmos RSA, Diffie-Hellman y criptografía de curvas elípticas.

No.	CONTENIDOS	HORAS AD Actividades de Docencia		HORAS TAA Actividades de Aprendizaje Autónomo		CLAVE BIBLIOGRÁFICA
		T	P	T	P	
3.1. 3.1.1 3.1.2	Conceptos de criptografía clave asimetrica Aplicaciones Ventajas y desventajas	1.5		1.0		1B,2B,3C,6B,7B, 8C,10C,11C
3.2. 3.2.1	RSA Seguridad y ataques a RSA	2.0	1.0	2.0	1.0	
3.3.	Algoritmo Diffie-Hellman	1.0	1.0	2.0	1.0	
3.4. 3.4.1	Criptografía de curvas elípticas (CCE) Ventajas y desventajas de CCE	3.0	1.0	2.5		
	Subtotales:	7.5	3.0	7.5	2.0	

ESTRATEGIAS DE APRENDIZAJE

La unidad temática se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico y comparativo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, discusión guiada y la práctica de laboratorio V.

EVALUACIÓN DE LOS APRENDIZAJES

Portafolio de evidencias:

Problemas resueltos	25%
Reporte de mesa redonda	5%
Evaluación escrita	35%
Elaboración de la práctica	35%
Autoevaluación y coevaluación (rúbrica)	

UNIDAD DE APRENDIZAJE: Criptografía

N° UNIDAD TEMÁTICA: IV **NOMBRE**: Fundamentos matemáticos de funciones Hash

UNIDAD DE COMPETENCIA

Genera aplicaciones criptográficas, con base en los algoritmos Hash: MD5 y SHA.

No.	CONTENIDOS	HORAS AD Actividades de Docencia		HORAS TAA Actividades de Aprendizaje Autónomo		CLAVE BIBLIOGRÁFICA
		T	P	T	P	
4.1	Introducción	0.5		0.5		2B,4B,6B,7B,8C, 9C,10C,11C
4.2	Características de las funciones Hash			0.5		
4.3	Algoritmo MD5	0.5		0.5		
4.4	Algoritmo SHA	0.5	1.0	1.0	1.0	
4.5 4.5.1 4.5.2	Aplicaciones de las funciones Hash Algoritmo de verificación de integridad de datos Algoritmos para firmas digitales	2.0	1.0		1.5	
	Subtotales:	3.5	2.0	2.5	2.5	

ESTRATEGIAS DE APRENDIZAJE

La unidad temática se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico y activo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, discusión guiada, trabajo de investigación, organizadores gráficos y la práctica de laboratorio VI.

EVALUACIÓN DE LOS APRENDIZAJES

Portafolio de evidencias:

Resolución de problemas	20%
Conclusión de debate	5%
Reporte de investigación	10%
Mapas mentales	5%
Evaluación escrita	35%
Reporte de la práctica	25%
Autoevaluación y coevaluación (rúbrica)	

UNIDAD DE APRENDIZAJE: Criptografía

Nº UNIDAD TEMÁTICA: V **NOMBRE**: Fundamentos matemáticos de firmas digitales

UNIDAD DE COMPETENCIA

Diseña programas de firmas digitales, con base en los algoritmos RSA, DSA y ECDSA.

No.	CONTENIDOS	HORAS AD Actividades de Docencia		HORAS TAA Actividades de Aprendizaje Autónomo		CLAVE BIBLIOGRÁFICA
		T	P	T	P	
5.1.	Conceptos de firmas digitales	1.5				1B, 2B,4B,3C,7B, 8C,9C,10C,11C.
5.2.	Proceso matemático de generación de firma, firmado y verificación de firma.	1.5				
5.3.	Firmas digitales con RSA.	1.0	0.5	1.0	1.0	
5.4.	Algoritmo de firma digital (DSA).	1.0	1.0	1.0	1.0	
5.5	Algoritmo de firmas digital con CCE (ECDSA)	1.5	1.0	1.0	1.0	
	Subtotales:	6.5	2.5	3.0	3.0	

ESTRATEGIAS DE APRENDIZAJE

La unidad temática se abordará mediante la estrategia de aprendizaje basado en problemas (ABP), el facilitador aplicará los siguientes métodos: analítico y comparativo. Las técnicas y actividades que auxiliarán a la estrategia seleccionada serán las siguientes: resolución de problemas, discusión guiada, programas de cómputo y la práctica de laboratorio VII.

EVALUACIÓN DE LOS APRENDIZAJES

Portafolio de evidencias:

Resolución de problemas	15%
Reporte de mesa redonda	15%
Evaluación escrita	35%
Reporte de la práctica	35%
Autoevaluación y coevaluación (rúbrica)	

UNIDAD DE APRENDIZAJE: Criptografía

RELACIÓN DE PRÁCTICAS

PRÁCTICA No.	NOMBRE DE LA PRÁCTICA	UNIDADES TEMÁTICAS	DURACIÓN	LUGAR DE REALIZACIÓN
1	Exponenciación binaria	I	2.0	Laboratorio de Telemática, Unidad y sitios fuera de la escuela
2	Algoritmo extendido de Euclides	I	2.0	
3	Implementación de AES en software	II	4.0	
4	AES en modo de operación	II	4.0	
5	Implementación de RSA	III	5.0	
6	Implementación de SHA	IV	4.5	
7	Implementación de ECDSA	V	5.5	
		TOTAL DE HORAS	27.0	

EVALUACIÓN Y ACREDITACIÓN:

Las prácticas se consideran requisito indispensable para acreditar esta unidad de aprendizaje.

Las prácticas aportan el 35% en las unidades temáticas I, II, III y V , y el 25% en la unidad temática IV. Esta evaluación se considera dentro de la evaluación continua.

UNIDAD DE APRENDIZAJE: Criptografía

PERÍODO	UNIDAD	PROCEDIMIENTO DE EVALUACIÓN
1	I y II	Evaluación continua 65% Evaluación escrita 35%
2	III y IV	Evaluación continua 65% Evaluación escrita 35%
3	V	Evaluación continua 65% Evaluación escrita 35%
		Los porcentajes con los que cada unidad temática contribuyen a la evaluación final son: La unidad I aporta el 20% de la calificación final. La unidad II aporta el 20% de la calificación final. La unidad III aporta el 20% de la calificación final. La unidad IV aporta el 20% de la calificación final. La unidad V aporta el 20% de la calificación final. Esta unidad de aprendizaje también se puede acreditar mediante: • Evaluación de saberes previamente adquiridos con base en los criterios que establezca la Academia. • Acreditación en otra unidad académica del IPN u otra institución educativa, nacional o internacional, externa al IPN, con la cual se tenga convenio.

UNIDAD DE APRENDIZAJE: Criptografía HOJA: 10 DE 11

CLAVE	B	C	BIBLIOGRAFÍA
1	X		Ferguson, Niels, Schneier, Bruce and Kohno Tadayoshi (2010). Cryptography Engineering: Design Principles and Practical Applications (1st Edition). USA: Wiley. ISBN. 978-0-470-47424-2.
2	X		Ferguson, Niels and Schneier, Bruce (2003). Practical Cryptography (1st Edition) USA: Wiley. ISBN: 0-471-22894-X.
3		X	Paar, Christof, Pelzl, Jan and Preneel, Bart (2010). Understanding Cryptography: A Textbook for Students and Practitioners (2nd Edition) Germany: Springer. ISBN 978-3-642-04100-6.
4	X		Schneier, Bruce (1996) Applied Cryptography: Protocols, Algorithms, and Source Code in C. (2nd Edition). USA: John Wiley & Sons inc. ISBN: 0-47111709-9.*
5		X	Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography (1st Edition). USA: Anchor books. ISBN: 0-385-49532-3.*
6	X		Wade Trappe, Lawrence C. Washington (2006). Introduction to Cryptography with Coding Theory (2nd Edition). USA: Pearson Prentice Hall. ISBN: 978-0-131-86239-5.
7	X		A. Mollin, Richard (2007), An Introduction to Cryptography (2nd Edition) USA: Taylor & Francis. ISBN: 978-1-58488-618-1.
8		X	Rhee, Man Young (2003). Internet Security: Cryptographic Principles, Algorithms and Protocols (1st Edition). UK: John Wiley & Sons. ISBN: 0-470-85285-2.
9		X	Hans Delfs, Helmut Knebl (2007), Introduction to Cryptography: Principles and Applications (2nd Edition). USA: Springer. ISBN: 978-3-540-49243-6.
10		X	Franklin, Mathew (Marzo 2012), Journal of Cryptology, from: http://www springer com/computer/theoretical+computer+science/journal/145
11		X	Landwehr, Crl E. (Marzo 2012), IEEE Security & Privacy, from: http://ieeexplore.ieee org/servlet/opac?punumber=8013
			* Libro clásico.

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

upiita·ipn

1. DATOS GENERALES

UNIDAD ACADÉMICA: UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERIA Y TECNOLOGÍAS AVANZADAS.

PROGRAMA ACADÉMICO: Ingeniería Telemática **NIVEL** III

ÁREA DE FORMACIÓN:

Institucional	Científica Básica	Profesional	Terminal y de Integración
		■	

ACADEMIA: Telemática **UNIDAD DE APRENDIZAJE:** Criptografía

ESPECIALIDAD Y NIVEL ACADÉMICO REQUERIDO: Maestría en sistemas de información o área afín

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE: Genera sistemas informáticos seguros con base en algoritmos criptográficos, tanto en software como en hardware y en sus protocolos.

PERFIL DOCENTE:

CONOCIMIENTOS	EXPERIENCIA PROFESIONAL	HABILIDADES	ACTITUDES
Programación avanzada Teoría de números Esquemas de cifrado simétrico y asimétrico Firmas digitales Protocolos de seguridad Modelo Educativo Institucional (MEI)	Dos años de experiencia mínima profesional en el campo de la Ingeniería en sistemas de información seguros Un año de experiencia impartiendo clases a nivel licenciatura y/o dos años impartiendo cursos o talleres.	Manejo del idioma inglés (avanzado) Dominio de la asignatura Manejo de grupos Comunicación oral y escrita Capacidad de análisis y síntesis Manejo de materiales didácticos Organización Creatividad Liderazgo Uso de las TICs Aplicar el MEI	Vocación por la docencia Honestidad Crítica Respeto Ética profesional y personal Responsabilidad Trabajo en equipo Superación docente y profesional Solidaridad Compromiso social y ambiental Responsabilidad Tolerancia Puntualidad, entre otros.

ELABORÓ	REVISÓ	AUTORIZÓ
Presidente de Academia Dr. Itzamá López Yáñez	M. en C. Jorge Fonseca Campos Subdirector Académico	M. en C. Arodi Rafael Carvallo Domínguez Director

INSTITUTO POLITÉCNICO NACIONAL
UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERÍA Y TEC. AVANZADAS
DIRECCIÓN